(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 117 124**
A2

(12) EUROPEAN PATENT APPLICATION

(21) Application number: **84300976.2**

(22) Date of filing: **15.02.84**

(51) Int. Cl.³: **G 07 F 7/10**

(30) Priority: **18.02.83 JP 25728/83**

(43) Date of publication of application:
29.08.84 Bulletin 84/35

(84) Designated Contracting States:
AT DE FR GB

(71) Applicant: **FUJITSU LIMITED**
1015, Kamikodanaka Nakahara-ku
Kawasaki-shi Kanagawa 211(JP)

(72) Inventor: **Kuroki, Akira**
1405, Omaru
Inagi-shi Tokyo 206(JP)

(72) Inventor: **Ochiai, Satoru**
1405, Omaru
Inagi-shi Tokyo 206(JP)

(74) Representative: **George, Sidney Arthur et al,**
GILL JENNINGS & EVERY 53-64 Chancery Lane
London WC2A 1HN(GB)

(54) Transaction safety system.

(57) A portable transaction device (31) having an input keyboard (36) is connected via a telephone line (34) to a data processing centre (35), which processes input data, fed from the transaction device relating to client transactions. The transaction device sends an alarm signal (E) in response to entry of an alarm code by the operator if the operator is having to carry out a false transaction under duress. Renewal of a client's file (46) at the data processing centre is prevented when the alarm signal is received at the centre so that the false crediting of funds to the client's account is prevented. A false funds-received processing text (G) is sent back to the transaction device so that a printer (45) enters details on the client's passbook (37) as though the transaction had been carried out normally. The system therefore allows the operator to indicate that he has made a false entry under duress and the data processing centre can take action to ensure that the falsely-credited funds cannot be withdrawn by the client. On the other hand, because the passbook shows an apparently normal updating of his credit, the client is not alerted to the fact that an alarm has been given. The likelihood of release of the operator unharmed is thereby greatly increased.

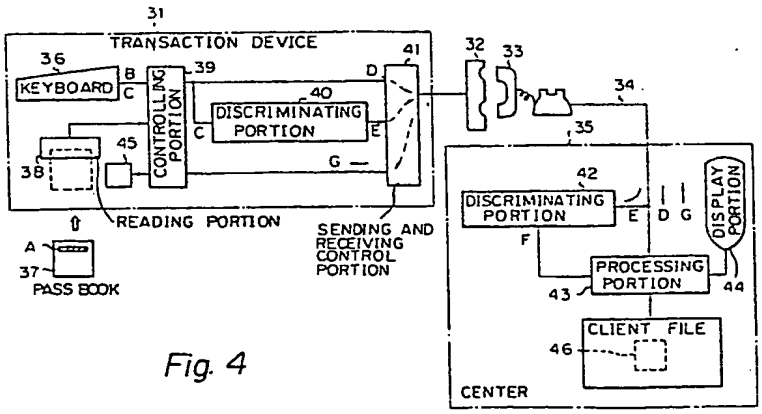


Fig. 4

EP 0 117 124 A2

Croydon Printing Company Ltd

BNSDOCID: <EP 0117124A2>

FUJITSU LIMITED 31/2094/02

TRANSACTION SAFETY SYSTEM

This invention relates to a transaction safety system for securing the safety of a monetary transaction in a system for monetary circulation.

When the staff of banks etc., visit clients to carry out a monetary transaction, they carry a portable monetary transaction device. This enables the staff to carry out the processing of any monetary transaction with their clients immediately from the client's premises, and a passbook in which a deposited value and a balance are printed out is delivered to the client on the spot. This portable monetary transaction device is connected, via an acoustic coupler and a telephone line, to a central processing unit so that the monetary transaction process (the process of indicating that funds have been received) is carried out immediately the central processing unit receives the input data. After the monetary transaction process is completed, data sent back from the central processing unit is printed out in the passbook by a printer incorporated in the device. This processing by a portable monetary transaction device is normally carried out by the client-liaison staff of a bank, and there is always a possibility of the staff being forced by a person with criminal intent, whether at the client's premises or during the journey to visit the client, to carry out the processing of a false receipt of non-existent funds. That is, to be forced to print out in the bank passbook an amount received without receiving this amount. Such a crime cannot be prevented by the conventional monetary transaction systems.

An object of the present invention is to prevent the above-mentioned criminal act from succeeding, and to provide a transaction safety system for securing the

BNSDOCID: <EP 0117124A2>

safety of a monetary transaction in a system for monetary circulation.

According to one aspect of the present invention there is provided a safety system for a transaction system in which a transaction device having an input portion and a processing device having a client file are connected by a circuit so that the processing device processes data fed from the transaction device; the safety system being characterised by means in the transaction device for sending an alarm signal when an improper transaction is carried out; file control means in the processing device for preventing renewal of the client file when the alarm signal is received; and controlling means for operating the alarm signal sending means when special code data are received from the input section.

According to another aspect of the invention, a safety system for a transaction system in which a transaction device having an input portion and a processing device having a client file are connected by a circuit so that the processing device processes input data from the transaction device; characterised in that the transaction device comprises a distinguishing portion which distinguishes whether or not the data input from an input portion comprises predetermined special code data; and sending means which sends an alarm signal in response to detection by the distinguishing portion of the input of the special code data; in that the processing device comprises alarm generating means which generates the alarm when the alarm signal is received from the transaction device; and means for sending back the text concerning the transaction device; and in that when the alarm signal is generated from the transaction device, the transaction device sends back the text as in a normal

transaction so that the transaction in the transaction device is completed.

Thus, as is clear from the above, in the event that the client liaison staff of a bank, when carrying a portable monetary transaction device, are forced by a person of criminal intent to process the receipt of non-existent funds, the staff can secretly feed a special code, such as (99 * 99), into the transaction device during the process of operating the device, i.e. during the process of inputting the funds-received data (account number, funds received, etc.) as part of the regular monetary transaction process. The central processing unit which receives the special code will not renew the account file, and will send back a false funds-received processing text (funds received, renewed balance etc.) in such a way that the criminal will assume that the file has been renewed. That is, the data are printed out in the bank passbook by the monetary transaction device, which receives the false funds-received processing text as if the processing of the funds received is completed in a normal manner, thereby ensuring the safety of the client-liaison staff. Later, when the criminal attempts to withdraw funds from the bank by using the false funds-received processing text printed out in the passbook, not only will it be impossible to withdraw funds from the bank, but also the fact that a crime has been committed will be exposed.

An embodiment of the invention will now be described, by way of example, with reference to the accompanying drawings, in which

Figure 1 is a block schematic diagram of a system for monetary transaction in which the present invention is applied;

Figure 2 is a pictorial view of a portable terminal forming part of the system;

Figure 3 shows a keyboard arrangement in the transaction safety system;

Figure 4 is a block diagram of the transaction safety system according to the present invention;

Figure 5 is a block diagram showing a configuration of the transaction device shown in Figure 4;

Figure 6 is a block diagram showing a configuration of a data processing centre in the system of Figure 4;

Figure 7A shows a client file and Figure 7B shows an error log file, both used in the apparatus of Figure 6;

Figures 8A and 8B are block diagrams illustrating one example of an ordinary deposit receipt/payment operation;

Figure 9A is a flow chart illustrating the operation of the system for a monetary transaction; Figure 9B is a flow chart showing the inputting of the data of the transaction into the terminal side shown in Figure 9A; and

Figure 10 is a flow chart illustrating the operation of the system for the monetary transaction in the centre side shown in Figure 9A.

Figure 1 shows the system for monetary transaction in which a host computer 1, a relay computer 2, a network control unit 3, and a client file 4 are provided in the main office of a bank or business centre, and a modem 5, a terminal controller 6, a portable terminal connection unit 7, a portable writer 8, a telephone adapter 9, and a network control unit 10 are provided in a branch office of the bank. A telephone exchange 11 is connected to the main office and to the branch office of the bank, and is further connected to a subscriber's telephone 12 (or via a subscriber's telephone 13) to a portable terminal 14. This portable terminal 14 corresponds to the transaction device according to the present invention.

In the system shown in Figure 1, the portable writer 8 has the same functions as the portable terminal 14

BNSDOCID: <EP 0117124A2>

provided in the branch office of the bank. The telephone exchange 11 can be connected either via the branch office of the bank or directly to the host computer 1.

As mentioned previously, because the portable terminal 14 is carried by the client-liaison staff of the banks, there is always a risk that the staff will be forced into processing the false receipt of non-existent funds, during a period when the staff are on the client's premises or when travelling between the bank and those premises.

Figure 2 is an external view of the portable terminal shown in Figure 1. Figure 2 shows an electric power source (i.e. a battery) 21, an acoustic coupler 22, a printer inserter 23, a liquid crystal display 24, a magnetic card read-out portion (a magnetic passbook read/write portion) 25 and a keyboard portion 26.

Figure 3 shows a keyboard arrangement for the portable terminal shown in Figure 2. The keyboard arrangement includes a digit key portion 29 and a function key portion 30.

Figure 4 is a block diagram of a transaction safety system according to the present invention. In Figure 4, a transaction device 31 includes a keyboard 36, a read portion 38 which reads a passbook 37, a control portion 39, a discriminating portion 40, and a sending and receiving control portion 41. The output of the transaction device 31 is coupled via a acoustic coupler 32 and a telephone handset 33 to a telephone line 34 and a data processing centre 35.

The centre 35 includes a discriminating portion 42, a processing portion 43, a display portion 44, and a client file 46.

Figure 5 shows a block diagram of the construction of the transaction device 31 shown in Figure 4. As shown in Figure 5, the control portion 39 and the discriminating

BNSDOCID: <EP 0117124A2>

portion 40 include a transaction control program, an input/output control program, a work area, a sending and receiving buffer, an identification storing portion, an SOS text, an input/output funds counter, and a journal record portion (for recording an account, an item, an amount, a name, and a centre number). The control portion 39, the discriminating portion 40, and a sending and receiving portion 41

are connected via a memory access controller 49 to a computer bus line. The computer bus line is connected via a display control 48a to a liquid crystal display portion 48. This connection is made via a control buffer 38a to a magnetic strip read/write portion 38, via a port 36a to a keyboard 36, via a printer control portion 45a to an inserter printer 45, via a line control portion 32a to an acoustic coupler 32, and via an input/output port 47a to a clock 47.

Figure 6 shows a block diagram of the construction of the center 35 shown in Fig. 4. As shown in Fig. 6, the processing portion 43 includes a computer, a transaction management program, a terminal identification, an operator identification, and a work area. A keyboard display 44 is formed by a liquid crystal display, and a client file shown in Fig. 4 is formed by an ordinal client file 46a and an error log file 46b. The center 35 is connected via a telecommunication control portion 50 to a telephone line 34.

The client file 46a is formed, as shown in Figure 7A, by an account number, an address, a name, a balance, and unrenewed data. The error log file 46b is formed, as shown in Figure 7B, by a defective account number, such as an accident, card lost, or a defective item, etc. The client-liaison staff of a bank carry this portable monetary transaction device 31 as shown in Fig. 4, when visiting a client. When, during such a visit, the client proposes the transfer of funds to the bank (for example a deposit), the bank staff connects this portable monetary transaction device 31 to the center 35, so as to input the desired data and to process the amount of funds received to the center 35. Thus the passbook, in which the funds received is printed out and recorded, can be delivered to the client immediately. Figures 8A and 8B are block diagrams showing the operation of an ordinary receipt/payment process. As shown in Figs. 8A and 8B, the input process (for example a

time deposit) is as follows:

(1) Selection of the item: specifying a fixed time deposit

(2) Reading the passbook: inserting the passbook into a reading portion and reading an identification code.

(3) Inputting a deposit number: inputting a code indicating the deposit number and "NOTE I."

(4) Inputting a transaction code: inputting the transaction code.

(5) Inputting a tax classificatin: inputting the numerical data and "NOTE II."

(6) Inputting a data of maturity: inputting the data giving the maturity date.

(8) Inputting a transaction classification: specifying that the interest is added to the principal, etc.

(9) Inputting funds received: inputting the data showing the amount of funds received.

In the event that the client-liaison staff of the bank encounter a person with criminal intent and are forced to process an imaginary amount of funds received, if the staff refuse to carry out this false processing, there is a great possibility that the personal safety of the staff will be endangered. Under this kind of pressure, obviously the staff will be obliged to connect the portable monetary transaction device 31 to the center 35 and input the data to the center 35 in accordance with the above process (1) ~ (9) by operating the keyboard 36.

According to the present invention, in such a case the predetermined special code (SOS code, for example "99 * 99") is secretly input when the input of process (3) or (5) is carried out. This prevents any access to the client file 46 in the center 35. At the same time, the data for the false funds received is printed out in the passbook 37, and the passbook is delivered to the

criminal.

In Fig. 4, after the client-liaison staff of the bank has operated the keyboard 36, e.g. to specify a fixed time deposit, the passbook 37 is inserted into the reading portion 38 of the monetary transaction device 31 in order to read out the identification code A. Next, when the deposit number code B is input from the keyboard 36, the special code C (for example, "99 * 99") is input. This special code C is fed via a control portion 39 to a discriminating portion 40. When the discriminating portion 40 discriminates this special code C, the discriminating portion 40 outputs an alarm signal E. Except for inputting the special code C, the client liaison-staff proceed to input the data in accordance with the input processes ① ∿ ⑨ above. When the input of the data is completed, a sending and receiving control portion 41 sends the data of the false funds received D (in accordance with processes ① ∿ ⑨) and the alarm signal E to the center 35. In the center 35, when the alarm signal E is included in the received data, a discriminating portion 42 discriminates this alarm signal E, and a control signal F is sent to a processing portion 43. When the processing portion 43 is determined as being in an abnormal state by a control signal F, the client account file 46 concerning the data of the funds received is not accessed, and a display portion 44 displays that an abnormal state has occurred. After that, the funds received, processing text G, which indicates that the processing concerning the funds D received is normally carried out, is sent back to the monetary transaction device 31. In the monetary transaction device 31, the funds received processing text G received in the sending and receiving portion 41 is sent to the controlling portion 39, so that a printer 45 prints out the data of the funds received and the data of the renewed balance etc., in the passbook 37. The client-liaison staff of the bank can thus escape from a

BNSDOCID: <EP 0117124A2>

difficult position by delivering this passbook to the person who has forced the staff to input an imaginary amount of funds.

When the criminal tries to withdraw the funds by using this passbook, in which the input of the funds is written, the crime is immediately discovered, as an abnormal condition data is registered in the bank computer system concerning the account number of this passbook.

Figure 9A is a flow chart of the operation of the monetary transaction system. Block 91 confirms the registration of the operator and, when the operator is registered, the transaction data is input to block 92, and sent to the center side by block 93. In the center side, a block 94 examines the transaction and the account file is renewed in block 95, where the special code (SOS code) is processed. In block 96, the processing text is drafted and sent to a received text process 97 in the terminal side. The processed text in the block 97 is printed out in block 98 and the processing is ended.

Figure 9B is a flow chart showing the input of the transaction in Fig. 9A. An input data of a transaction input 100 is buffered in block 101 (a sending buffer), is monitor displayed in block 102, and the displayed item is examined in block 103 to determine whether or not it is a function key operation. When the item is a function key operation, the output of block 103 is sent to block 104 where it is examined to determine whether or not the special code is included. When the special code is included, it is set in the sending buffer 101. When the special code is not included in block 104, the numeric data is checked in block 106. When the numeric data is good, the monitor is erased in block 107, and the data of the input buffer and the function key data is set in the sending buffer in block 108. The input data is compiled and displayed in block 109, and is examined to determined whether or not the input is

complete in block 110. When the input is complete, the data is fed to the coupler in block 111. In block 112, the data is then sent to the center. When block 106 judges that the numeric data is defective, an error processing is effected via block 113.

Figure 10 is a flow chart showing the operation in the center side. Data is received in block 120, and block 121 then determines whether or not an error is included in the received data. When an error is included in the data, an error message is added in block 122. When an error is not included, the data is examined in block 123 to determine whether or not the special code (SOS text) is included. When the special code is included in the data, the account number thereof is stored in the error log file in block 124, and an alarm is displayed in block 125. When a special code is not included, the identification and the operator of the input data are checked in block 126. When the data checked in block 126 is defective, an alarm is displayed in block 127, and an imaginary (error) text is drafted in block 128 and sent out.

When the data checked in block 126 is good, the transaction is checked in block 129. If the result of the data check in block 129 is defective, the imaginary (error) text is drafted in block 130.

When the result of the data check in block 129 is good, the account file is renewed in block 131, and the text is drafted in block 132. When the text is drafted in block 132, the amount of the false funds received is included in the text.

The text drafted in block 132, the error message drafted in block 122, and the error text drafted in block 130 are sent to the terminal via the send process in block 133.

As mentioned previously, according to the present invention, when forced to carry out the processing of a false amount of funds received in the monetary

transaction, by using the portable monetary transaction device, the client liaison staff can inform the center of an abnormal status while processing a transaction seemingly in a normal manner, keeping this fact secret from the criminal, and ensuring the personal safety of the staff. This will also prevent the criminal from later withdrawing the false funds from the bank.

CLAIMS

1. A safety system for a transaction system in which a transaction device (31) having an input portion (36) and a processing device (35) having a client file (46) are connected by a circuit (32,33) so that the processing device processes data fed from the transaction device; the safety system being characterised by means (40) in the transaction device for sending an alarm signal (E) when an improper transaction is carried out; file control means (42, 43) in the processing device for preventing renewal of the client file when the alarm signal is received; and controlling means (39) for operating the alarm signal sending means when special code data are received from the input portion.

2. A system according to claim 1, characterised in that the transaction device comprises an input portion (36) which inputs transaction data concerning a transaction required by a client; an output portion (40, 41) which outputs the result of the transaction carried out in accordance with the input transaction data; a connecting portion (32, 33) which connects the transaction device to the processing device via a subscriber's telephone line (34); and a case which stores the input portion, the output portion, and the connecting portion, and which is portable.

3. A system according to claim 1 or claim 2, characterised in that the transaction device (31) comprises a discriminating portion (40) which discriminates whether or not the input data includes predetermined special code data, and the means (41) for sending the alarm signal is actuated in response to detection of the predetermined special code data.

4. A system according to any preceding claim, characterised in that the transaction device (31) comprises buffer means (39) which temporarily stores the

BNSDOCID: <EP 0117124A2>

input transaction data from the input portion; means (41) for collectively sending the transaction data (D) stored in the buffer means when the input of the transaction data concerning unit transactions is completed; and controlling means (40) which stores the predetermined type of alarm signal in the buffer means when the predetermined special code signal is received; and in that the alarm signal (E) is sent together with the transaction data (D) stored in the buffer means to the processing device by the sending means.

5. A system according to claim 3, characterised in that the special code data is included in the transaction data which is necessary to the transaction of a deposit using a passbook (37), and the discriminating portion (40) discriminates whether or not the special code data (C) exists in the transaction data which is input during the transaction.

6. A system according to claim 2, characterised in that the output portion includes a printing device (45) which prints and outputs the result of the transaction on to a passbook (37); and in that the printing device prints the content of the transaction based on the text (G) output from the processing device (35) and sent via the subscriber's telephone line (34).

7. A system according to any preceding claim, characterised in that the processing device (35) comprises discriminating means (43) which discriminates whether or not the required transaction included in the transaction data sent out from the transaction device is correct; detecting means (42) which detects the alarm signal in the received data; alarm output means including a display device (44) which outputs the alarm signal; and means for sending a response text (G) for the received transaction data to the transaction device.

8. A safety system for a transaction system in which a transaction device (31) having an input portion (36) and a processing device (35) having a client file (46) are connected by a circuit (32,33) so that the processing device processes input data from the transaction device; characterised in that the transaction device comprises a distinguishing portion (40) which distinguishes whether or not the data input from the input portion comprises predetermined special code data; and sending means (41) which sends an alarm signal in response to detection by the distinguishing portion of the input of the special code data; in that the processing device comprises alarm generating means (42) which generates the alarm when the alarm signal is received from the transaction device; and means (43) for sending back the text concerning the transaction device; and in that when the alarm signal is generated from the transaction device, the transaction device sends back the text as in a normal transaction so that the transaction in the transaction device is completed.

9. A system according to any preceding claim, characterised in that the transaction device (31) comprises a circuit connecting portion (32) which communicates the transaction device with the processing device (35) via a subscriber's telephone line (34); a printer (45) which types and outputs the result of the transaction on to a passbook (37) so that the result of the transaction is printed and output in accordance with text (G) sent back from the processing device (35) via the circuit.

10. A system according to claim 9, characterised in that the transaction device (31) comprises buffer means for buffering the transaction data (B) input from the input portion (36); sending means (41) for sending the data stored in the buffer means in accordance with the completeness of the transaction data concerning unit

BNSDOCID: <EP 0117124A2>

transactions to the processing device as the required transaction data (D); and controlling means (39) which sends out the alarm signal to the sending means when predetermined special code data (C) is input and which types and outputs the result of the transaction on to the passbook (37) regardless of the input of the special code data in accordance with the text (G) sent from the processing device.

11. A system according to claim 8 or claim 9, characterised in that the processing device (35) comprises controlling means (43) which renews the client file (46) based on the transaction data received from the transaction device (31) and which inhibits renewal of the client file when the alarm signal (E) is included in the data; and send back means which sends back the text (G) including the result of the transaction in accordance with the received transaction data to the transaction device (31) regardless of the presence of the alarm signal.

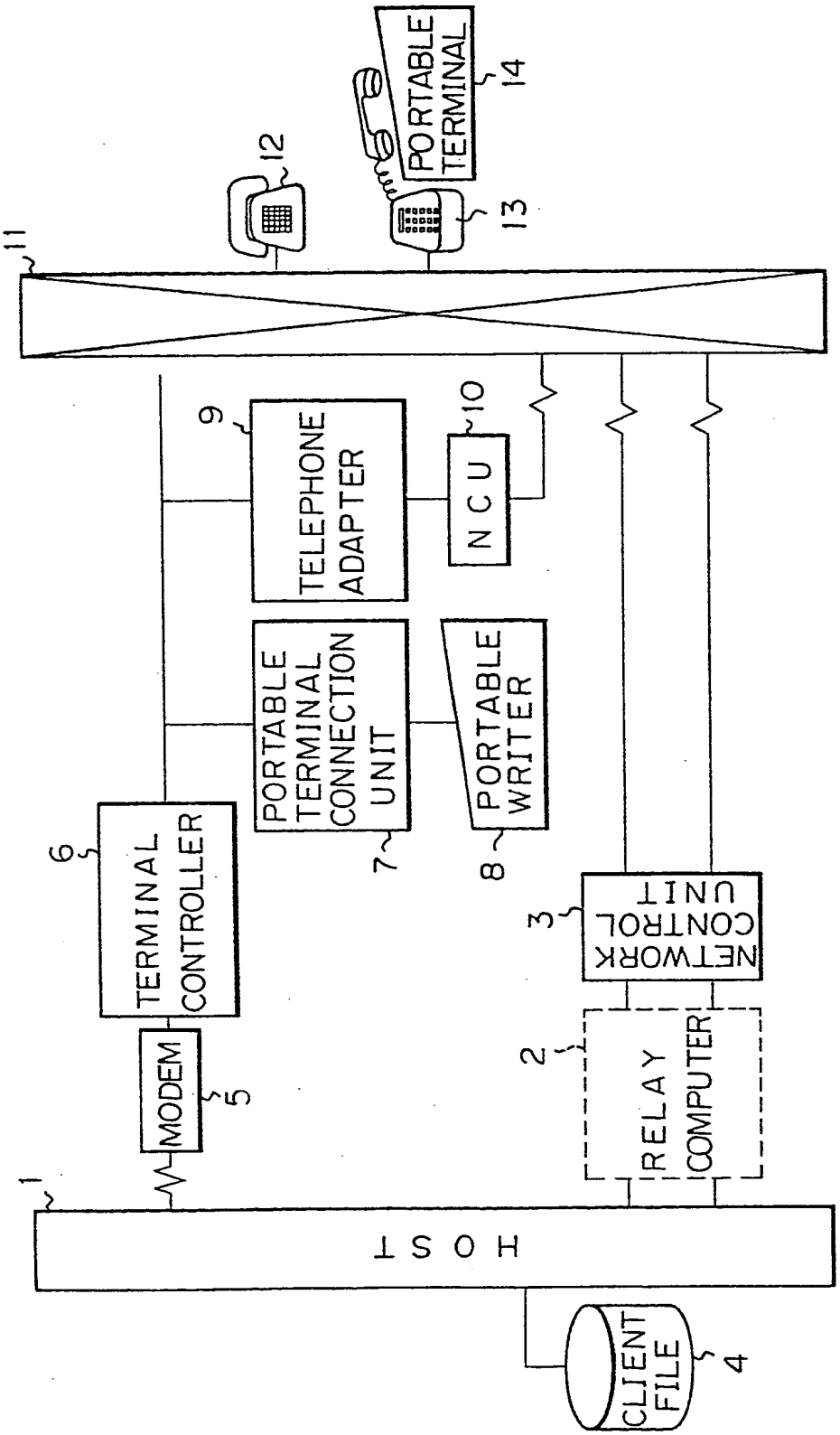
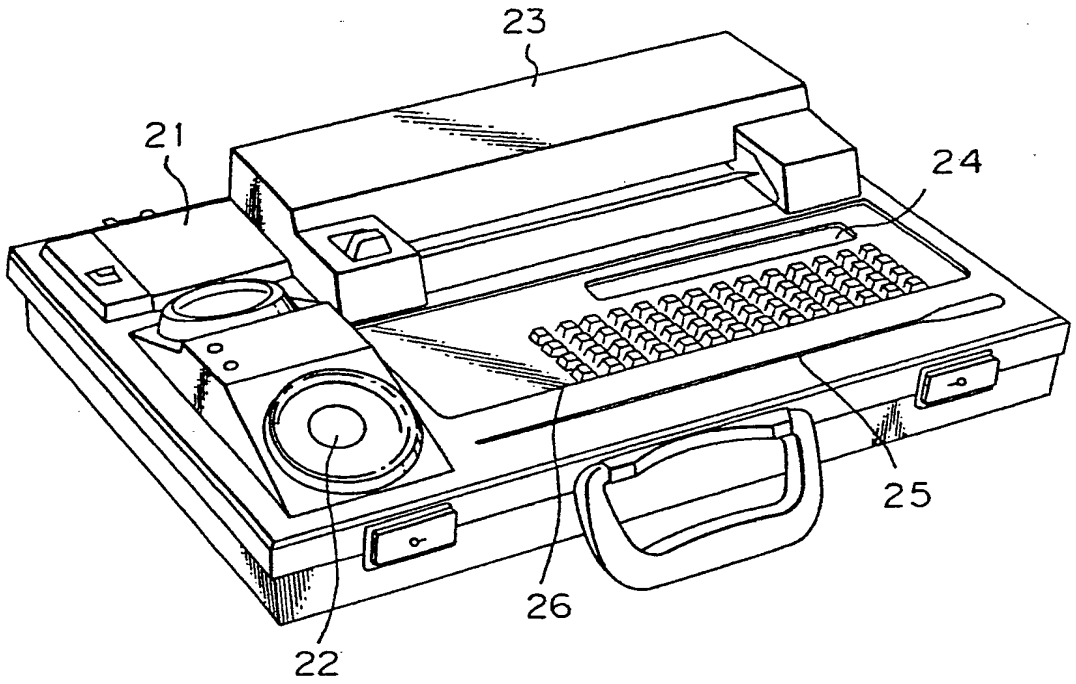


Fig. 1

BNSDOCID: <EP 0117124A2>

Fig. 2



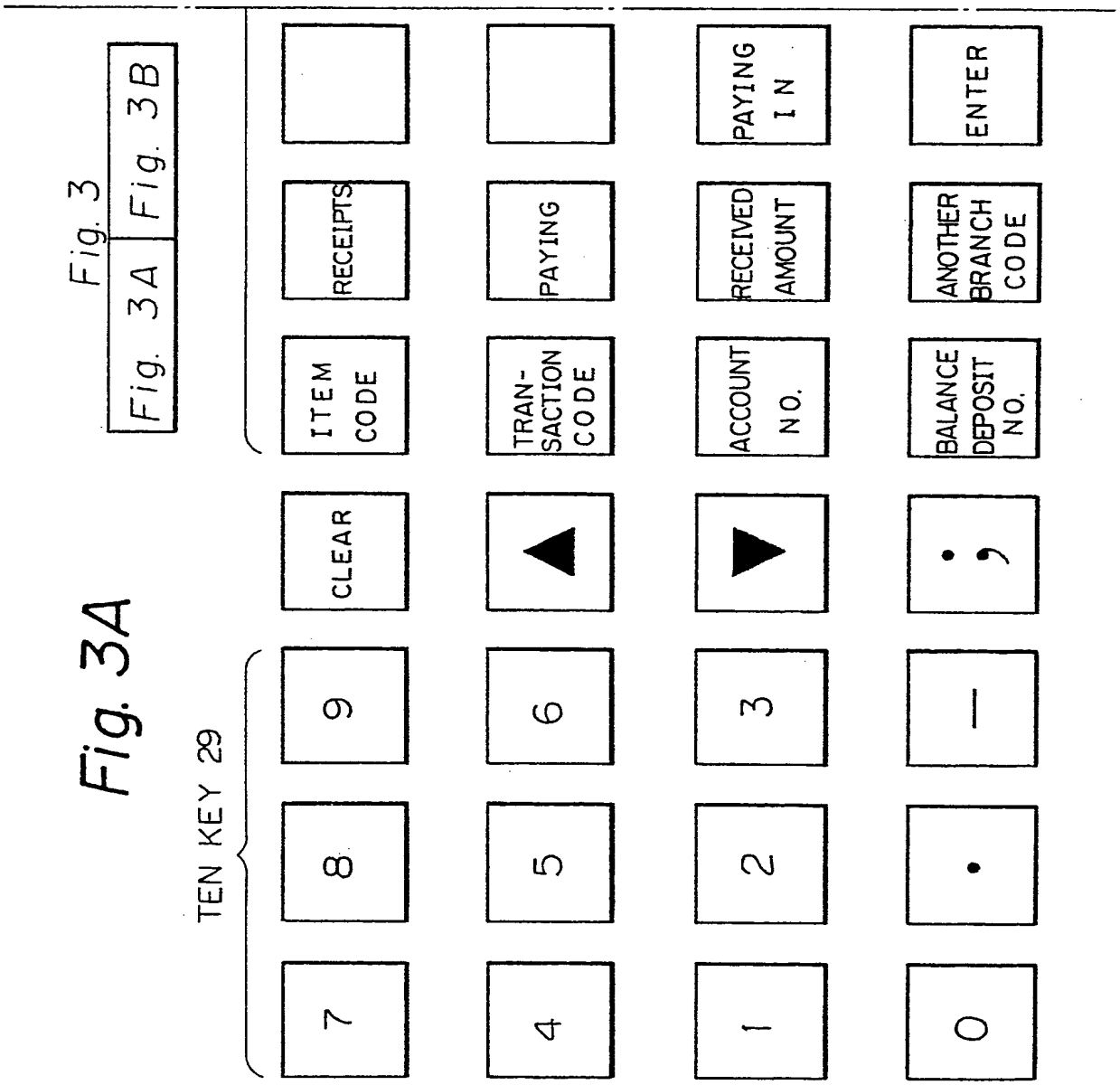
BNSDOCID: <EP 0117124A2>

0117124

Fig. 3

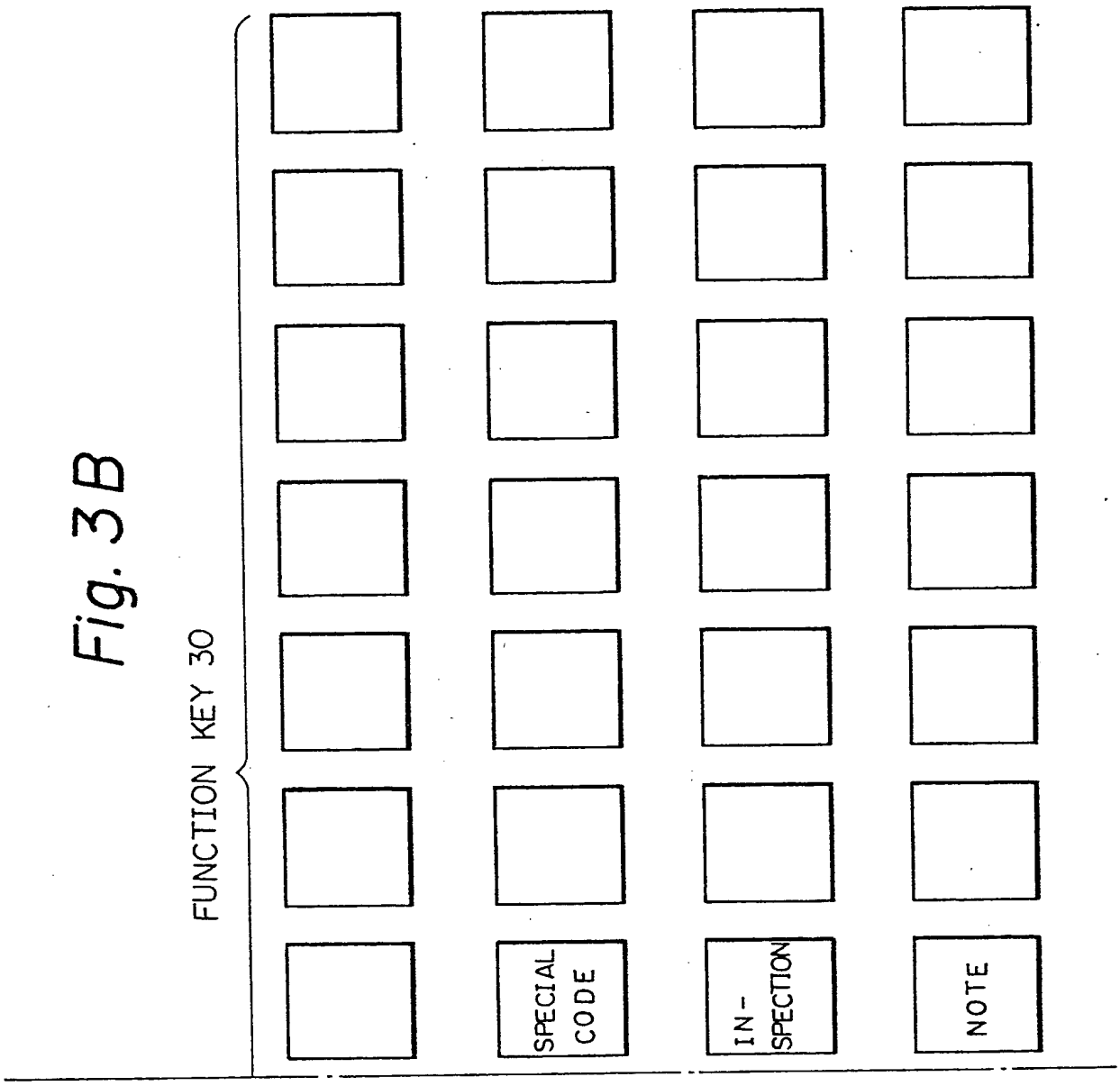
Fig. 3A	Fig. 3B

Fig. 3A



BNSDOCID: <EP 0117124A2>

Fig. 3B



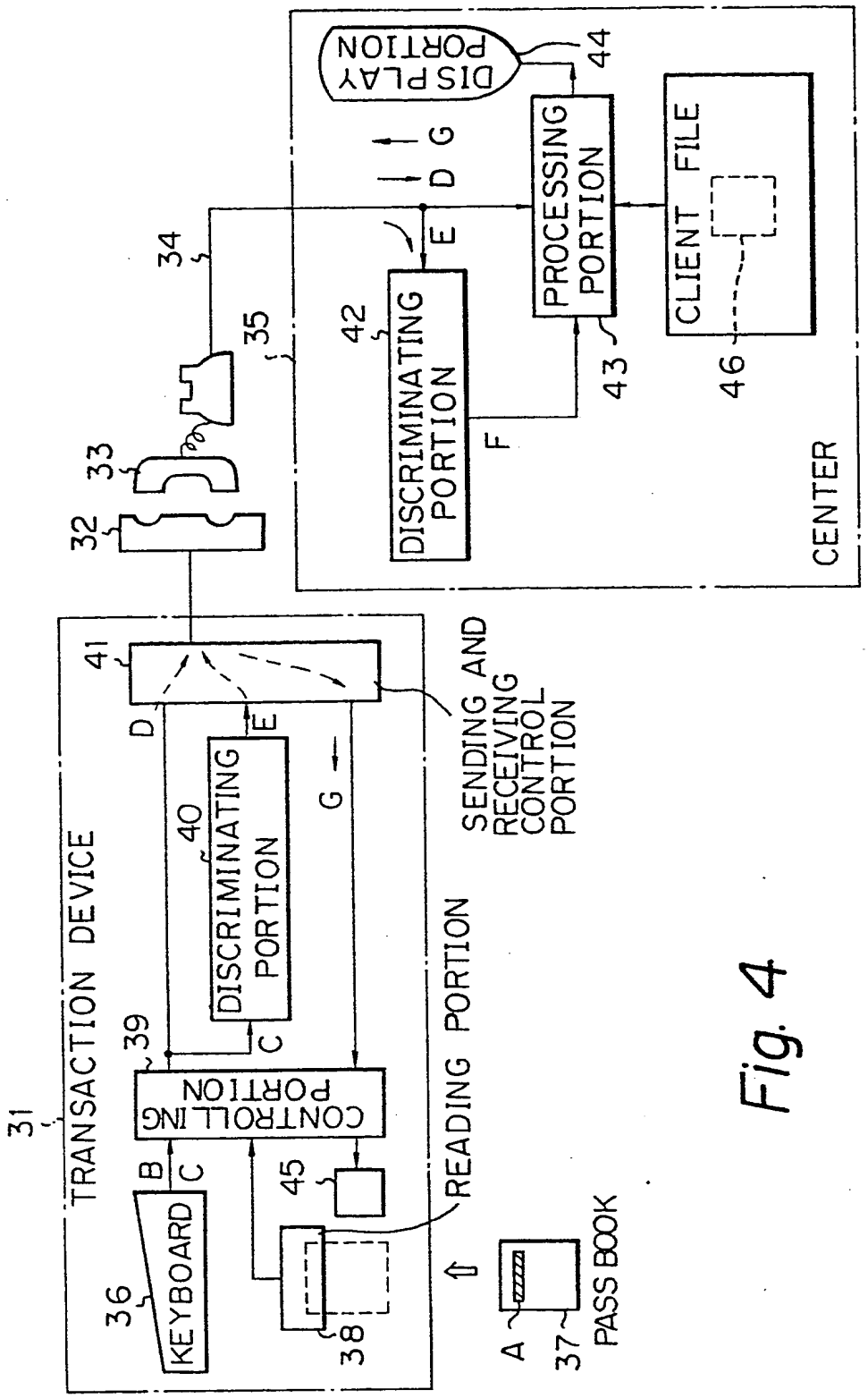


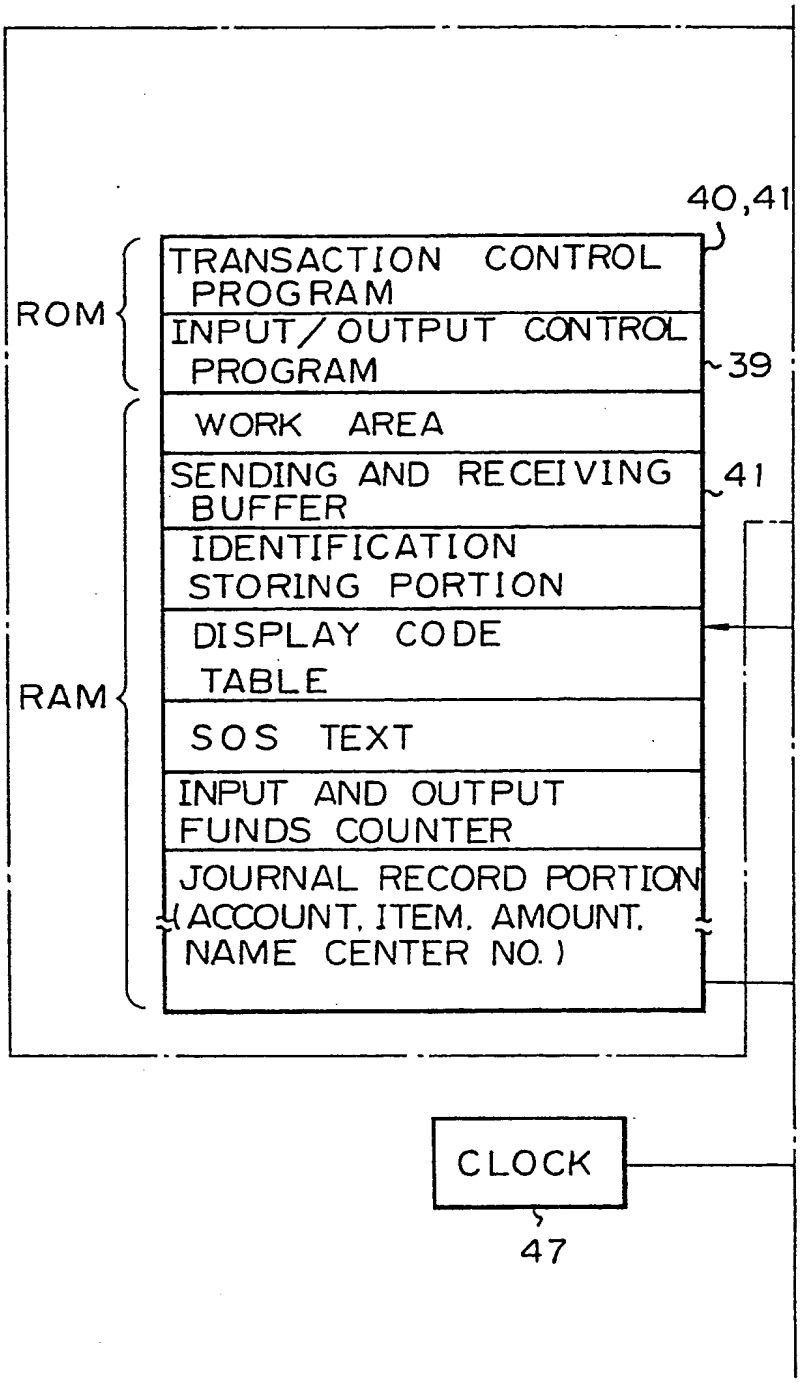
Fig. 4

BNSDOCID: <EP 0117124A2>

Fig. 5

Fig. 5A	Fig. 5B

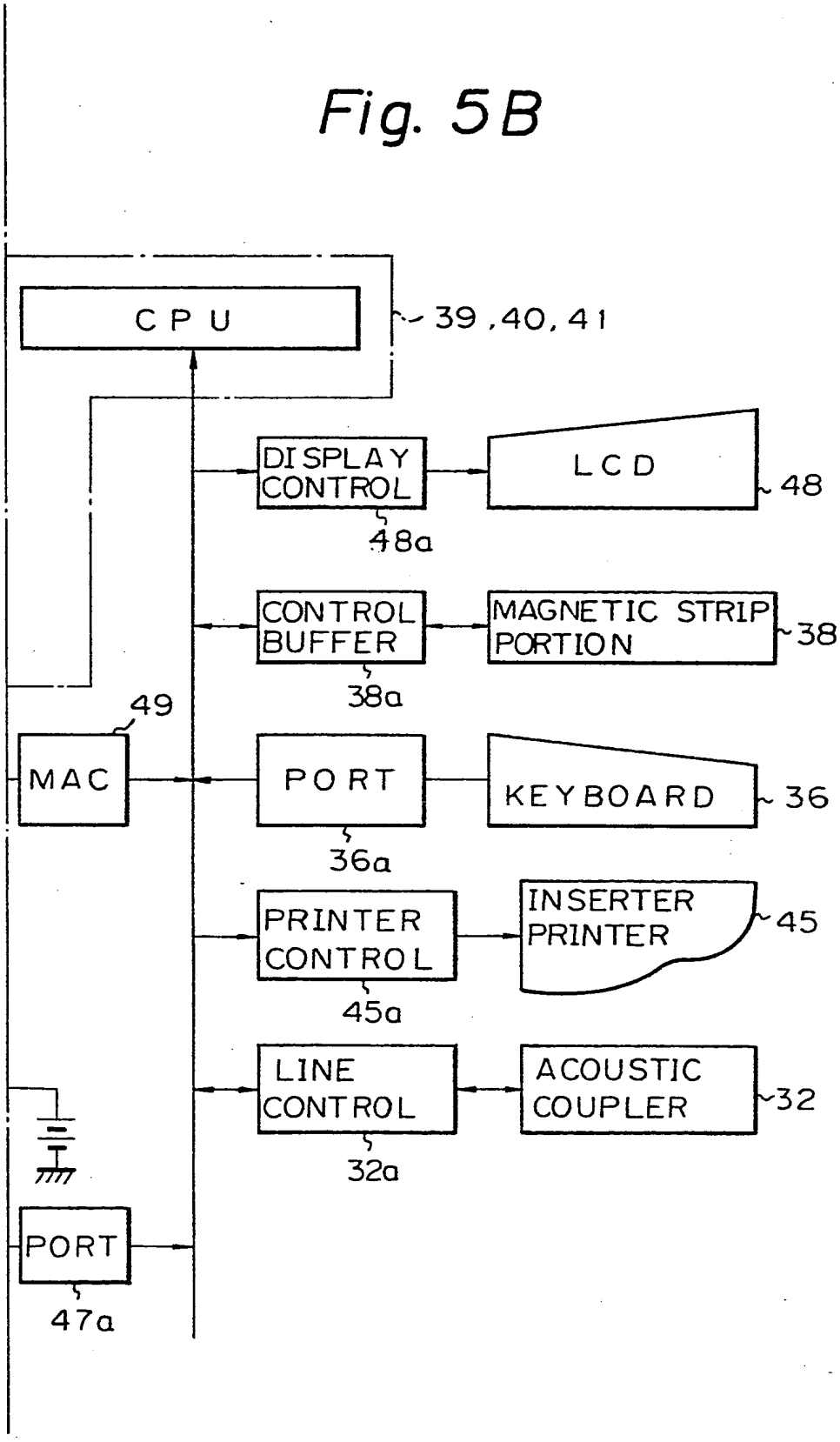
Fig. 5A



BNSDOCID: <EP 0117124A2>

0117124

Fig. 5B



BNSDOCID: <EP 0117124A2>

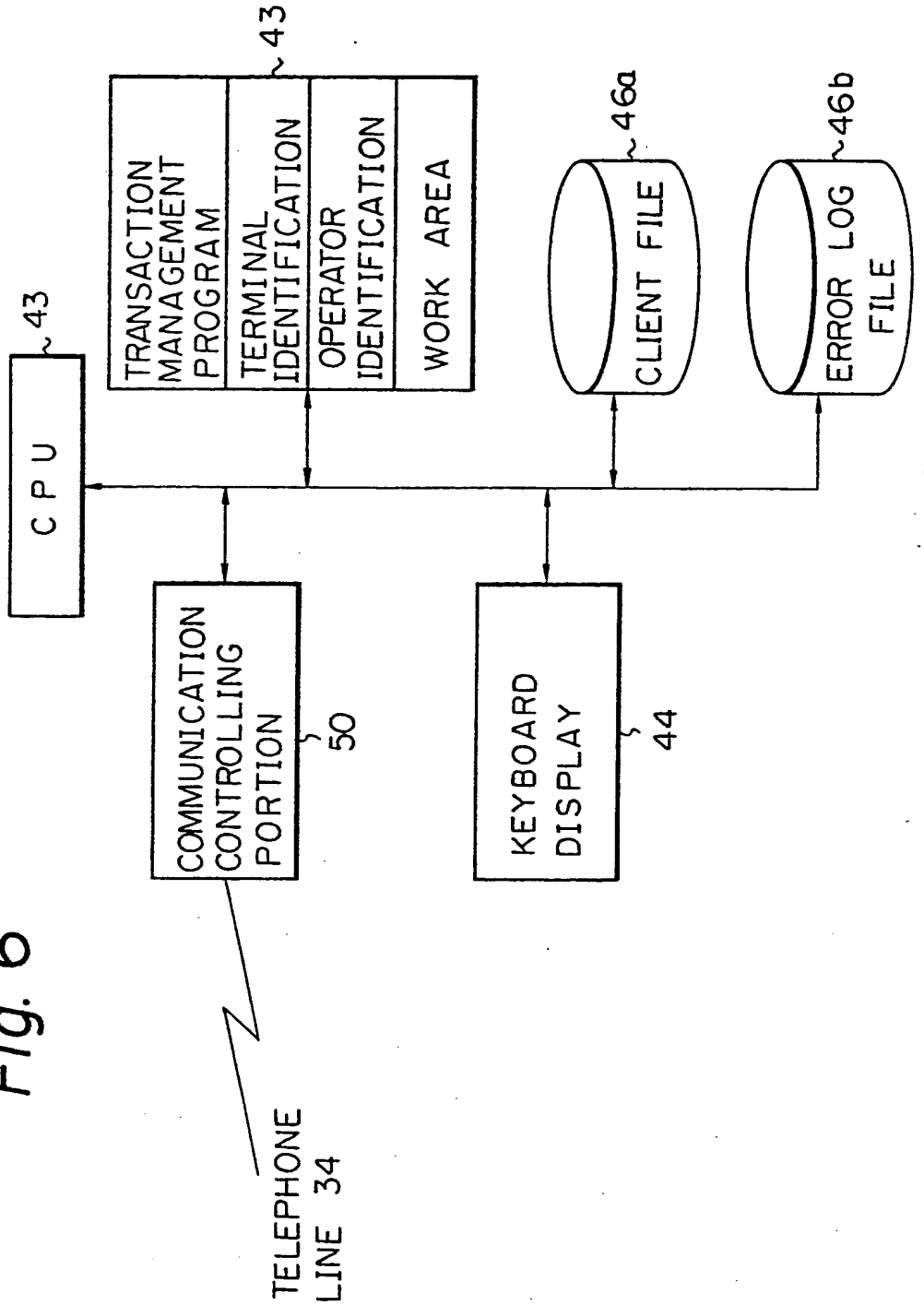


Fig. 6

BNSDOCID: <EP 0117124A2>

Fig. 7A

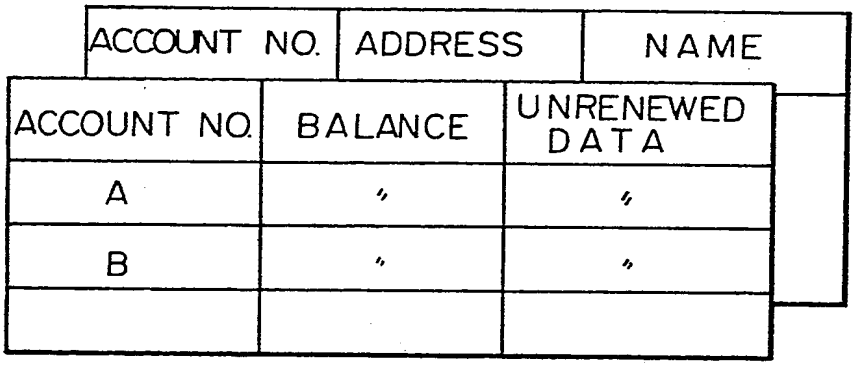


Fig. 7B

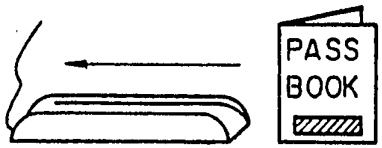
DEFECTIVE ACCOUNT NO.	ACCIDENT, CARD LOST, DEFECTIVE ITEM
A	
B	

BNSDOCID: <EP 0117124A2>

Fig. 8A-1

Fig. 8A

Fig. 8A-1
Fig. 8A-2

	KEYBOARD / PASSBOOK INPUT	DISPLAY
(1) SELECTS THE ITEM	02 ITEM CODE	ITEM CODE 02
(2) READS THE PASSBOOK M S	 PASS BOOK	ACCOUNT NO. 1231234567
(3) ENTERS THE DEPOSIT NO.	03 005 NOTE DEPOSIT NO. CODE	NOTE 1 03005
(4) ENTERS THE TRANSACTION CODE	016 TRAN-SACTION CODE	TRANSACTION CODE 016 TAX CLASSIFICATION

0117124

BNSDOCID: <EP 0117124A2>

Fig. 8A-2

(5) ENTERS THE TAX CLASSIFICATION	3	ENTER	TAX CLASSIFICATION 3 TERM
(6) ENTERS THE TERM	24551	ENTER	TERM 24551 DATA OF MATURITY
(7) ENTERS THE DATE OF MATURITY	840401	ENTER	DATE OF MATURITY 84-04-01 CLASSIFICATION
(8) ENTERS TRANSACTION CLASSIFICATION	1	ENTER	CLASSIFICATION 1
(9) NO ITEM ENTERED SKIPS	ENTER		CLASSIFICATION 1 INITIAL DATE

11/18

Fig.8B
Fig.8B-1
Fig.8B-2

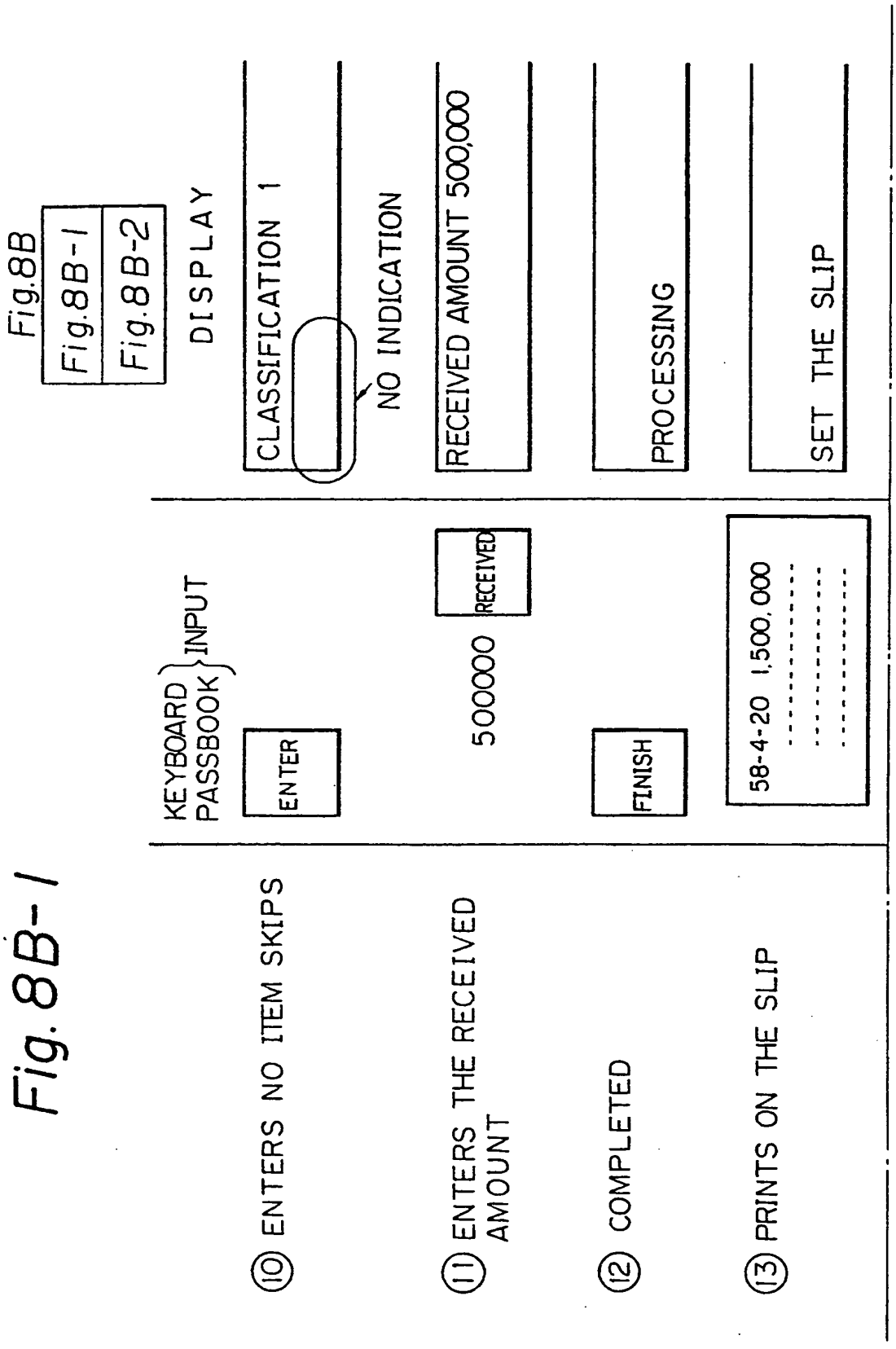


Fig. 8B-1

BNSDOCID: <EP 0117124A2>

BNSDOCID: <EP 0117124A2>

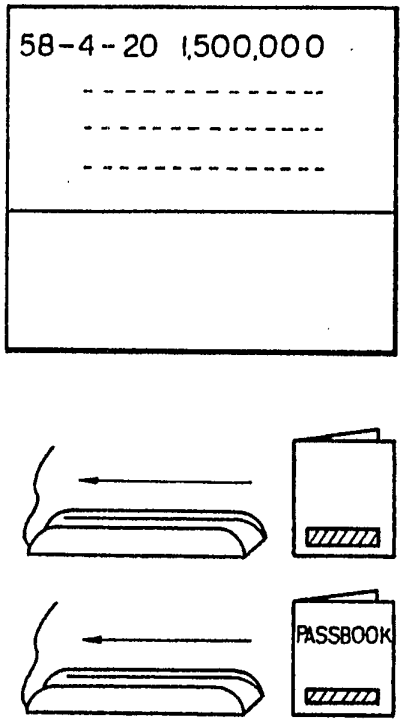
Fig. 8B-2

(14) PRINTS ON THE PASSBOOK

(15) WRITES THE MS OF THE PASSWORD

(16) REREADS THE MS OF THE PASSWORD

(17) INDICATES THAT THE TRANSACTION HAS BEEN COMPLETED NORMALLY



EXTRACT MATERIAL

SET PASSBOOK

EXTRACT MATERIAL

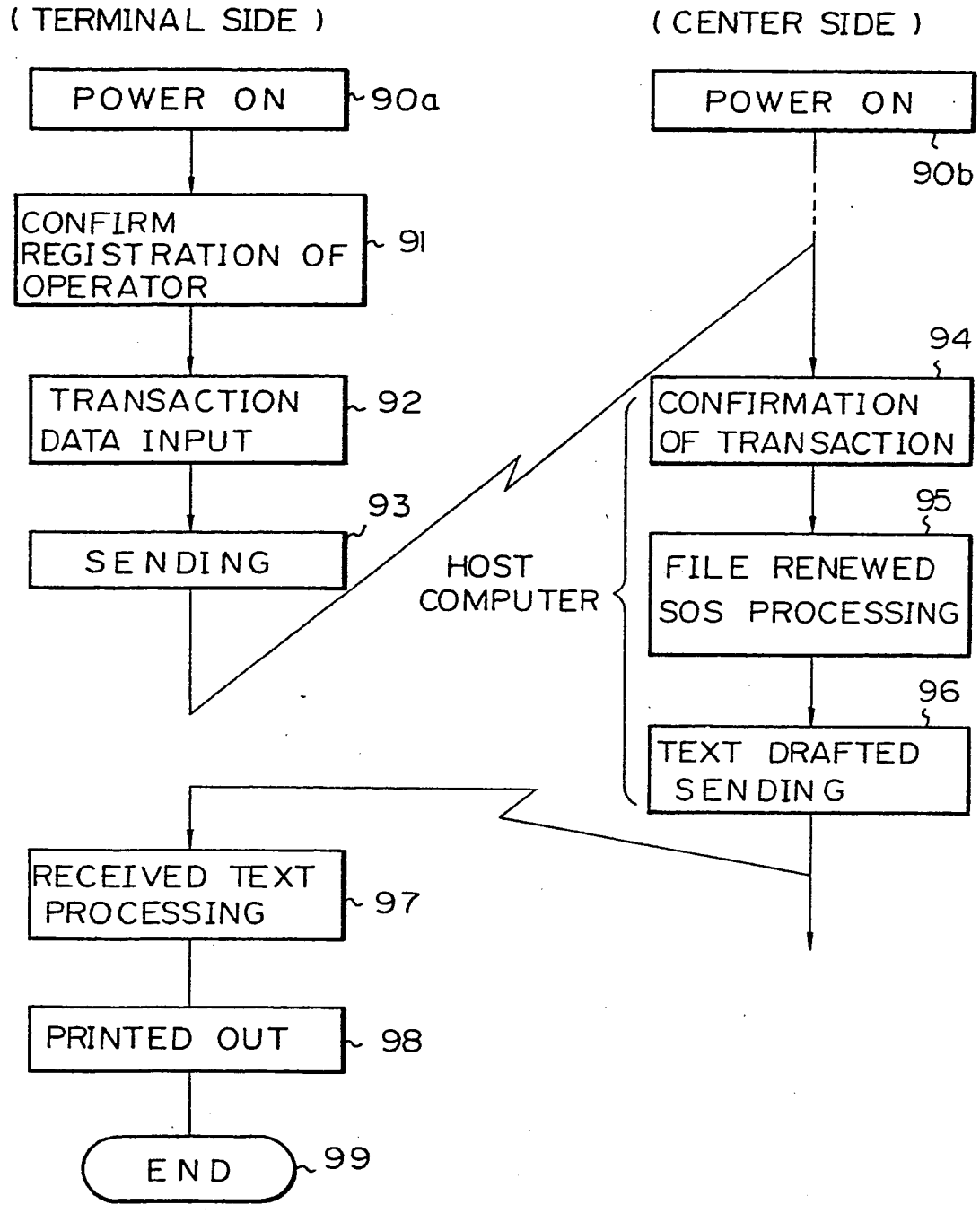
WRITE TO ME PASSBOOK

READ THE PASSBOOK

END OF OUTPUT

0117124

Fig. 9A

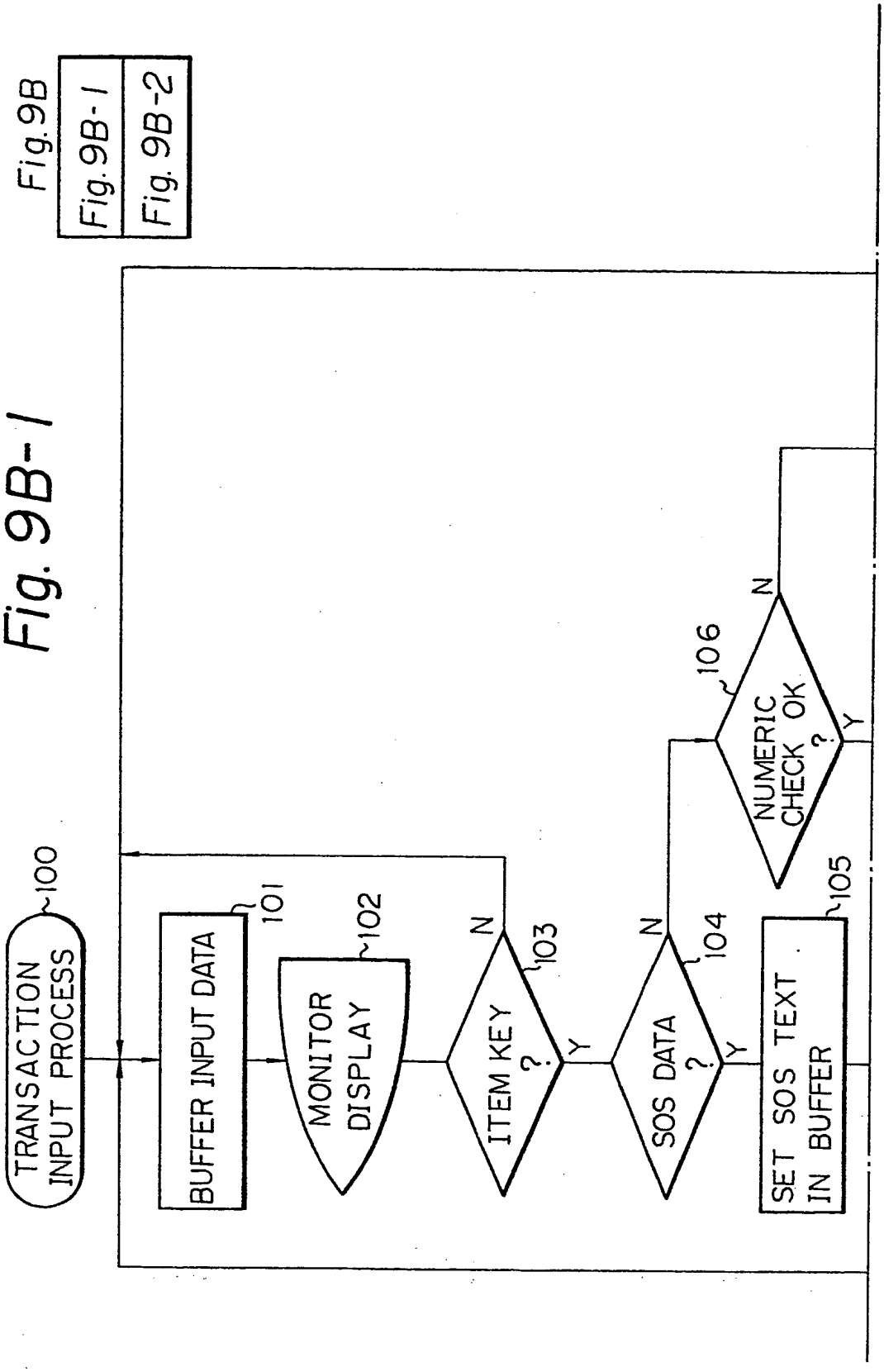


BNSDOCID: <EP 0117124A2>

Fig. 9B

Fig. 9B-1	Fig. 9B-2

Fig. 9B-1



BNSDOCID: <EP 0117124A2>

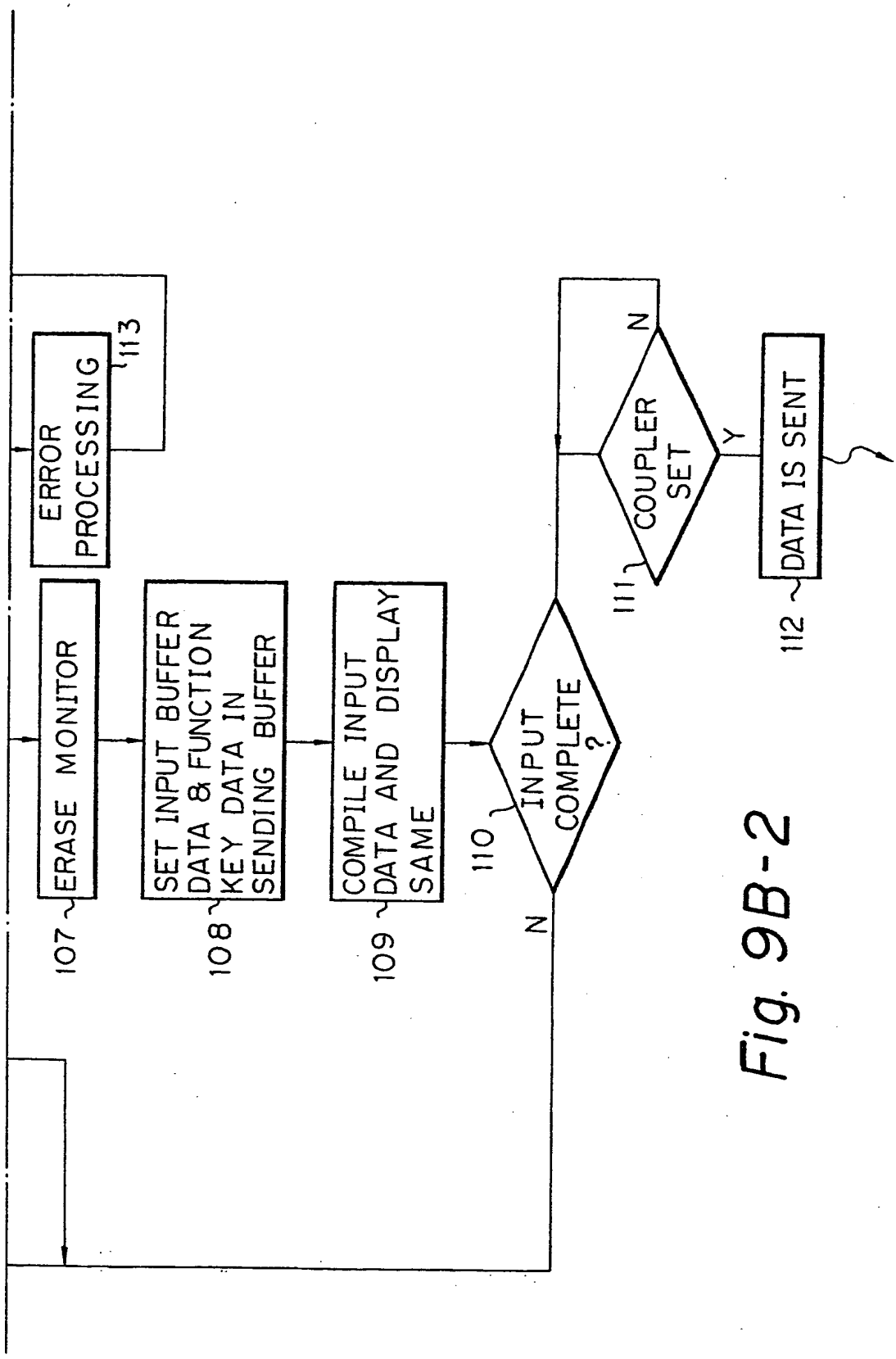


Fig. 9B-2

BNSDOCID: <EP 0117124A2>

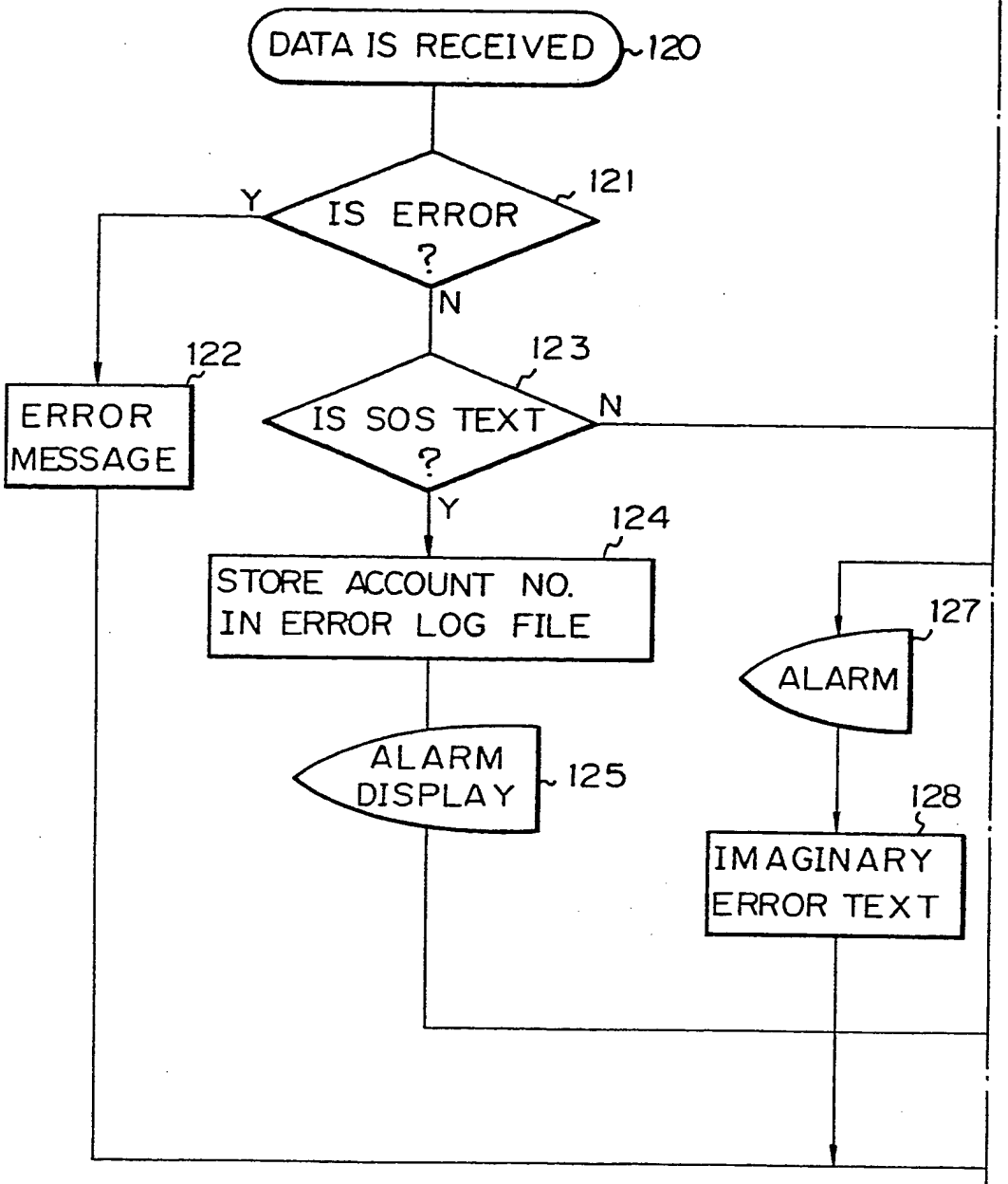


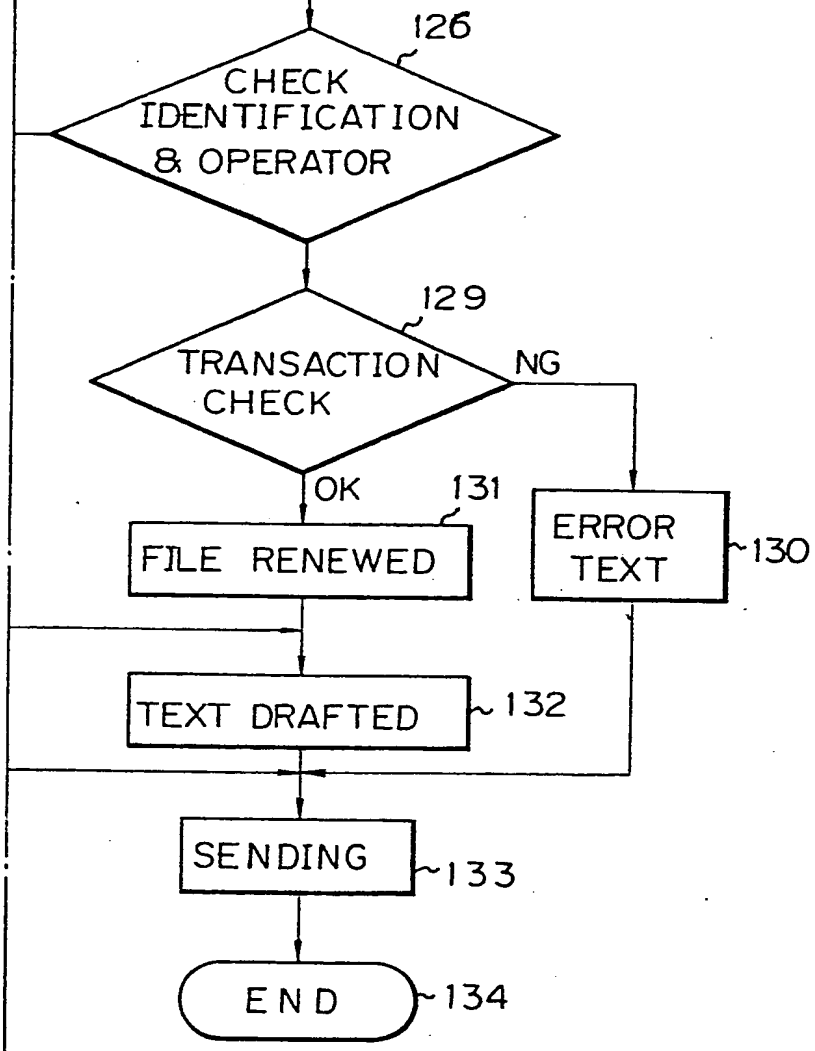
Fig. 10A

Fig. 10

Fig. 10A	Fig. 10B

BNSDOCID: <EP 0117124A2>

Fig. 10B



BNSDOCID: <EP 0117124A2>

THIS PAGE BLANK (USPTO)